Can Privacy and Security Be Friends? A Cultural Framework to Differentiate Security and Privacy Behaviors on Online Social Networks

Ersin Dincelli
College of Engineering & Applied Sciences
University at Albany, SUNY
edincelli@albany.edu

Sanjay Goel
School of Business
University at Albany, SUNY
goel@albany.edu

Abstract

The boundaries between online privacy and security behaviors in the literature seem blurred. Although these two behaviors are conceptually related, we argue that one does not necessarily imply the other. In this study we aimed to (1) explore the subtle differences between online privacy and security behaviors, and (2) examine how users' cultural characteristics and a group of multi-level factors exert different effects on the two behaviors. To achieve these two goals, we created a framework by coupling the grid-group theory and INDCOL scale to segment individuals into four categories based on autonomy (individualist vs. collectivist) and acceptance of control (hierarchy vs. equality). The results of one-way ANOVA and path analysis partially confirmed that the underlying mechanisms of online privacy and security behaviors were inherently different. This study provides a basis for creating contextualized security trainings and warnings based on individual differences to promote better privacy and security behaviors.

1. Introduction

Online social networks (OSN) have contributed to large amounts of data being collected about individuals. A large part of the information collected through these platforms is voluntarily disclosed. Such voluntary disclosure of personal information on OSNs might put both individuals and organizations at risk of security and privacy related threats [21], such as inference attacks that involve ascribing identity (individual or organizational) to confidential information on OSNs by using re-identification algorithms [17]; social engineering attacks, such as spear-phishing [25], where highly contextualized emails are created based on information that is available on users' OSN profiles; and malware attacks [22] through malicious links on OSNs. Such threats need to be countered aggressively to mitigate information security risks, such as by employee training, security policies, and security reminders.

One of the most common techniques used to improve the security profile of an organization is security training, which is important for both improving employee capability and ensuring compliance. Thus far, a majority of the training has been standardized and provided uniformly to employees across the entire organization; these measures, however, have not been effective in sufficiently stemming organizational security breaches to reduce information security risks to acceptable levels, partly because individuals differ in the ways they learn and the same training applied uniformly across the entire population is not equally effective for all individuals. Contextualized training, security warnings, messages, and incentives based on individuals' perception of privacy and security have a higher chance of being effective in motivating employees to adopt better online security and privacy behaviors [27]. To contextualize trainings and warnings adequately, it is crucial to understand employees' online behaviors and attitudes regarding potential security and privacy issues. This may be particularly helpful in organizations with a culturally diverse workforce where employees have different motivations and attitudes toward security and privacy based on their culture and prior experiences.

It is also important to note that while security and privacy are often used interchangeably, there is a subtle distinction between them; different mechanisms exist for shaping behavioral intentions across each of these constructs. Privacy stems from the users' desire to keep their information to themselves to protect their image or to prevent other people from misusing their information. Security, on the other hand, is a need for individuals to protect themselves from potential losses that they could incur from different threats including disclosure of information. The calculus used to assess security and privacy behavior is different; consequently, in the context of security and privacy behaviors may differ as well.

In some cases, security and privacy behaviors are aligned. For example, individuals with the intention to protect their online security (e.g., use of complicated passwords, stricter security settings, and security software) may also value online privacy protection (e.g.,

URI: http://hdl.handle.net/10125/41645
ISBN: 978-0-9981331-0-2

disclosing personal information). In other cases, security and privacy behaviors may be in stark contrast. For instance, an OSN user might be highly conscious about his/her privacy and not reveal any information online, however, he/she may use a weak password to secure his/her accounts. The possible reasons for this neglect could be low levels of the perceived importance of good security behavior or lack of security knowledge. Therefore, although they are related, privacy and security behaviors should be studied as two distinct constructs.

This study examines the potential dichotomy between privacy and security behaviors, particularly information disclosure and password behaviors. We argue that online privacy and security behaviors are different as they may be influenced differently by factors across multiple levels and we investigate the role of intrapersonal and interpersonal factors in causing this difference. The paper is organized as follows. Section II discusses the differences between online security and privacy behaviors, and the cultural values that may explain this difference. Section III presents the research design and methodology. Section IV reports the analyses of various sub-hypotheses under our propositions and discusses the results. Finally, section V concludes the paper.

2. Literature review

2.1. Online privacy and security behaviors

Behavior is a complex construct and no single factor can solely explain a specific behavior. Several ecological models (e.g., the ecological model of health behavior [38] and the self-management model [19]) were developed to explain a mechanism where behavior is influenced by factors from multiple levels, such as intrapersonal (e.g., psychological and demographics, such as attitude and gender), interpersonal (e.g., cultural and social, such as norms, family, and group pressure), organizational, community, and policy factors [20]. Correspondingly, online privacy and security behaviors may be also affected by factors across multiple levels.

The confluence of multi-level factors in behavior determination makes the promotion of behavior change difficult. To achieve successful behavior change, it is necessary to understand the influence of these factors on narrow behavioral traits rather than broad classes of behavior where multiple behavioral traits are lumped together. For instance, privacy and security are often lumped together in behavioral research. However, although they are aligned in many ways, there are enough subtle differences between them that users can be differently influenced by different determinants in their decision making. For example, factors that influence an individual to adopt the use of a strong password may not be the same for protecting his/her personal information.

The theory of planned behavior (TPB) posits that individuals' behaviors are influenced by subjective norms (interpersonal) and attitudes (intrapersonal) [1]. TPB has been used to predict privacy and security related behaviors [36] [37] [50]. However, the influence of constructs from TPB on privacy and security behaviors within the same study has not yet been studied. In this work, we examine the distinction between the driving mechanisms of security and privacy behaviors. To begin, we will posit that security related behaviors are relatively more autonomous compared to privacy behaviors. For instance, the decision to use a strong password depends mainly on the self rather than others. This behavior is more under one's own control, but it may depend on factors, such as technical knowledge, experience, and computer literacy [44]. Additionally, there is anecdotal evidence based on personal interactions with others that people do not usually explicitly discuss their security settings or passwords with others. Such information is "hidden." Thus, in contrast to privacy related behaviors, such as disclosing daily activities on OSNs, one is less likely to be socially judged if he/she uses a weak password. Therefore, we can infer that behaviors that are related to security are more "intrapersonal" compared to privacy behaviors, which drives our first proposition:

Proposition 1: Intrapersonal factors, such as privacy concern and literacy, are more influential in shaping security behaviors compared to privacy behaviors.

Privacy behaviors, on the other hand, can be more influenced by interpersonal factors compared to security behaviors. For example, individuals may disclose sensitive personal information motivated by various reasons, such as forming desirable impression through online self-presentation, socializing, expressing oneself to others, meeting social expectations, or pleasing others [26]. Due to such motivations, the extent of privacy behaviors can be influenced by how individuals perceive others view them based on the information they disclose on OSNs. Online privacy behaviors are inherently more "interpersonal" compared to security behaviors because the decisions about content and the amount of online self-disclosure may be affected by individuals' perceptions of what others might think of them.

Proposition 2: Interpersonal factors, such as subjective norms, are more influential in shaping privacy behaviors compared to security behaviors.

There may exist antecedent variables that predict intrapersonal and interpersonal factors. We argue that cultural values may be possible influential antecedents that determine the level of influences that intrapersonal and interpersonal factors can impose on online security and privacy behaviors. The following sections will highlight individualism and collectivism as underlying cultural values, which refers to individuals' perspectives of autonomy and control.

2.2. Equality and hierarchy (control) vs. dependence and self (autonomy)

Cultural values may explain variations in various privacy and security related phenomenon [21]. In fact, the relationship between culture and individuals' online behavior as well as other relevant constructs (e.g., attitudes and intentions) has been well documented in the literature [34]. However, culture is a complex construct and many theoretical frameworks, most with similar underlying dimensions, have been proposed to examine the influence of culture [41]. One particular dimension used in these frameworks is individualism vs. collectivism refers to both "autonomy" and "collective patterns of behaviors (dependence)" [48]. This social outlook is a foundational element of our work because it can be applied to the examination of how and to what extent underlying intrapersonal and interpersonal factors influence and predict individual behavior.

Individualism refers to the individuals' preference for a loosely-knit social framework where, compared to collectivism, interaction with others are less cohesive and integrated [24]. Individualists value autonomy, freedom, and control over their own behavior. In the context of this study, individualists may consider that it is their own responsibility to take actions to improve their security and protect their privacy.

Proposition 3: Users who are more autonomous (e.g., individualists) are more likely to be influenced by intrapersonal factors (e.g., privacy concern and literacy), which may lead to stronger security behaviors.

In contrary, collectivism emphasizes social bonds, harmony, and close integration within a group. In collectivist societies, self is determined by membership within the group [24]. Hence, collectivists put less emphasis on individual control and greater emphasis on conforming to collective patterns of behaviors and loyalty within their group [5]. This may lead to a greater acceptance of the invasion of their privacy by the group members [46]. However, outside their group, collectivists may tend to prefer more implicit communication (e.g., hiding their identities and having less explicit user profiles on social media) compared to individualists [49]. Thus we propose:

Proposition 4: Users who are more interdependent (e.g., collectivists) are more likely to be influenced by interpersonal factors (subjective norms), which may lead to stronger privacy behaviors.

Proposition 5: Users who tend to have greater control over their behavior are more likely to have stronger security and weaker privacy behaviors.

Researchers have examined the effects of individualism and collectivism in the context of information security (e.g., security awareness and education) and privacy (e.g., self-disclosure and privacy concern). However, the findings were inconsistent and sometimes contradictory.

In the literature, it was assumed that individualists possess higher security awareness and knowledge compared to collectivists b they consider protecting their security personal responsibility. Kwak et al. [33] identified three constructs related to security, namely familiarity, awareness, and knowledge. They found that the effects of these constructs were significantly lower in South Korean compared to the U.S., which is a highly individualist society [24]. Similarly, Schmidt et al. [44] found that Chinese users had significantly low security awareness compared to users from the U.S. Chen et al. [8] conducted an experiment to test the effectiveness of different techniques used for security education and found that individualists were more receptive to security trainings.

Some results on the relation between individualism-collectivism and privacy are mixed. Bansal et al. [3] examined the intention to disclose health information online and did not find a significant effect of individualism on self-disclosure. Posey et al. [43] investigated the influence of individualism and collectivism on online community self-disclosure and found that the tendency toward collectivism increased online self-disclosure. However, in a similar setting, Krasnova and Veltri [31] and Krasnova et al. [32] found that information disclosure was significantly higher in higher levels of individualism. In addition, Krasnova and Veltri [31] found that the negative effect of privacy concern on self-disclosure was stronger in lower levels of individualism. Several studies found no significant effect of individualism on privacy concern [39] [4] [6]. However, Milberg et al. [40], and Lili and Min [35] found positive effect of individualism on privacy concern. In contrast, Lowry et al. [36] found a positive relationship between collectivism and privacy concern.

Such inconsistent and contradictory results could be addressed by expanding or refining theoretical frameworks and improving the methodology. Culture represents the sum of multiple elements including beliefs, values, and principles [34], and it can be conceptualized in various ways. Individual behavior is influenced by these elements and the different levels of culture concurrently, such as national, regional, organizational, and group cultures (e.g., religious and ethnic) [28]. Although cultural values are distinct, they are not mutually exclusive. Individuals may exhibit multiple cultural characteristics concurrently [45]. Therefore, categorizing individuals under broad cultural values may be misleading. In the following section, we propose a framework that can be adopted to segment individuals with distinct cultural characteristics on a two-dimensional spectrum for more accurate cross-cultural comparisons.

2.3. Grid-group theory and individualism-collectivism (INDCOL) scale

Douglas [14] proposed the grid-group theory to examine different worldviews—how people perceive the world around them and act upon this perception. The grid-group theory divides population into four types of social environments in which individuals are expected to behave: hierarchic, egalitarian, individualistic, and fatalistic. The four types of social environments are determined by the dynamics along two dimensions (i.e., the group and the grid) where individuals exhibit the same type of behavior at different levels. The grid-group theory is represented in Figure 1.

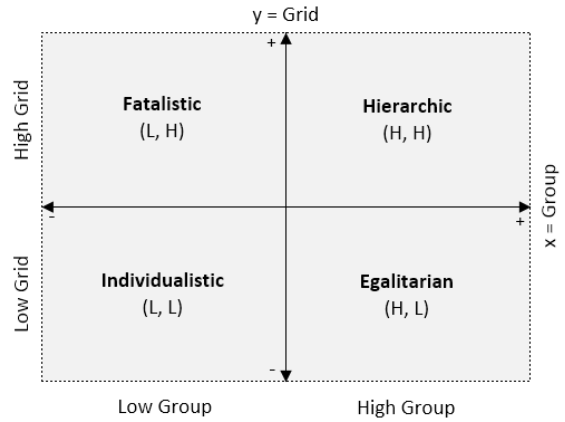

Figure 1. The grid-group theory

The group-axis (x-axis) represents the influence that the group exerts on the individual (i.e., how strongly people are bounded together), and the grid-axis (y-axis) is a measure of how much control an individual accepts from external resources (e.g., government, society, and group). The hierarchical environment, for example, shows a high degree of group influence and acceptance of control on individual behavior.

Singelis et al. [45] argued that there might be significant differences in understanding authority, hierarchy and equality, and they proposed two dimensions each of individualism and collectivism. Both horizontal individualism (HI) and vertical individualism (VI) recognize the full autonomy of a person. However, HI emphasizes equality, whereas VI accepts hierarchy and inequality among individuals. Horizontal (HC) and vertical collectivist (VC) identify the self as a part of the collective. However, HC recognizes equality among the individuals of the collective, whereas VC acknowledges hierarchy and inequality [48] [45]. The characteristics of each subcategory are shown in Table 1.

Both the grid-group theory and the INDCOL scale are used to create a taxonomy using conceptually related social outlooks. If the dimensions of INDCOL are placed

Table 1. Characteristics of Vertical and Horizontal Individualism and Collectivism

Vertical	Collectivism	Interdependent, low freedom Different than others, authority ranking, low equality, hierarchy
	Individualism	Independent, high freedom, autonomy Different than others, authority ranking, low equality, hierarchy
Horizontal	Collectivism	Interdependent, low freedom Same as others, equality matching, high equality
	Individualism	Independent, high freedom, autonomy Same as others, equality matching, high equality

in a two-axis system similar to the grid-group theory, we can represent individualism and collectivism on a two-dimensional spectrum where we can segment individuals based on the extent to which they possess different perspectives of control and autonomy.

Creating such segmentation would allow the comparison of individuals who possess distinct cultural values without mixing the sample with individuals who exhibit multiple cultural characteristics simultaneously. This would lead to more accurate group comparisons [11]. Figure 2 shows the tendency of each group to intrapersonal and interpersonal behaviors based on autonomy and acceptance of control.

The different levels of autonomy and acceptance of control vary in the dimensions of individualism and collectivism. Horizontal individualists have the most autonomy and the least acceptance of control over their behavior followed by vertical individualists, horizontal collectivists, and vertical collectivists respectively. As we discussed earlier, we can relate the extent of control one has over his/her behavior and interdependence to intrapersonal and interpersonal factors. In fact,

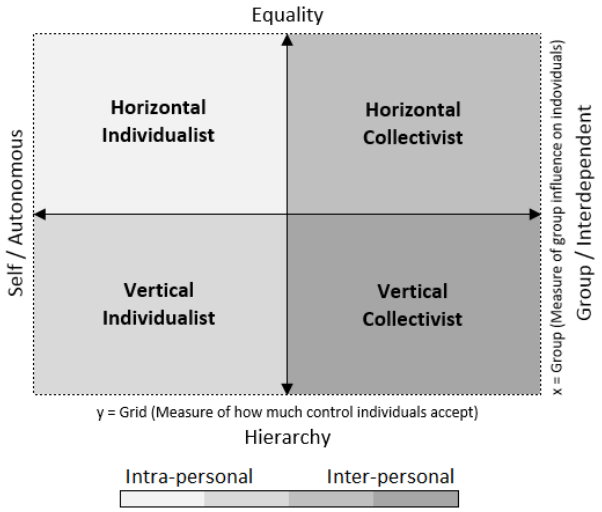

Figure 2. Dimensions of INDCOL and the degree of behavior based on autonomy and hierarchy

individuals who tend to accept hierarchy are more likely to give up their control over their actions to an authority [36]. This can also be true for the acceptance of invasion of privacy and low perceived importance of security. We will examine the differences across these groups in the context of online privacy and security behaviors.

Proposition 6: Online privacy and security behaviors are in contrast depending on individuals' control over their behavior and sense of autonomy.

2.4. Conceptual model

Several studies showed that models based on the TPB were efficient in predicting privacy and security related intentions and behaviors [36] [37] [50]. The TPB suggests that the intention to perform a behavior is the strongest predictor of the actual behavior [1]. Intention is determined by three factors: attitude, subjective norms, and perceived behavioral control (PBC). In order to test our propositions, we created a conceptual model that follows basic premises of the TPB

We adapted constructs from the TPB and integrated dimensions of INDCOL scale with interpersonal and intrapersonal factors, intention, and the behavior. We defined two specific behaviors to examine privacy and security behavior: Information disclosure and password behavior. We substituted attitude with privacy concern and PBC with Internet literacy. Figure 3 shows the relationships among the constructs in our model. We will explain each construct in the following section in detail.

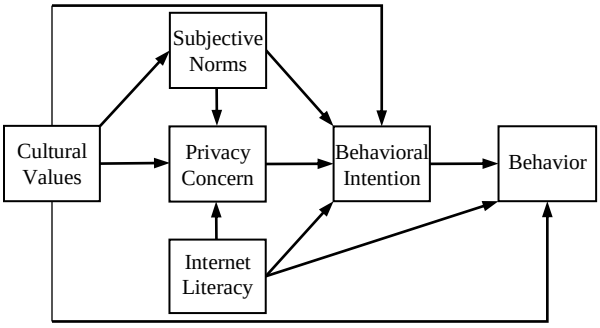

Figure 3. Conceptual model

3. Methodology

3.1. Measures

The survey included measures used to assess four dimensions of INDCOL scale, subjective norms, privacy concern on Facebook, Internet literacy, two behavioral intentions, and behaviors for both information disclosure and password. The survey items were adapted from previously validated instruments where possible. An expert panel and a pilot test (n = 76) were performed to validate the instruments before the final data collection. For both security and privacy behaviors, intention was measured using a single item: "I intend to change my Facebook password on a regular basis (at least once a year)" and "I intend to keep only my close friends and family members on my Facebook network." The INDCOL scale was measured using a five-point Likert scale. Other constructs were measured using seven-point Likert scales. The survey instruments are included in the online appendices due to space constraints.

3.1.1. Individualism-collectivism (INDCOL) Scale. The INDCOL scale consists of 16 items formed by four items per each subscale. Participants indicated their level of agreement by using a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The scores were determined by summing the items in each subscale. Higher scores indicated higher levels of the associated cultural value orientation (see Appendix A in the online appendices for the INDCOL scale).

3.1.2. Subjective norms. Subjective norms refer to an individual's perception and judgment of the normative expectations of specific salient others [1]. As suggested by the TPB, people are more likely to intend to perform behaviors that are approved by important referents [1]. Pressures due to subjective norms and peer behaviors were also found to influence employees' information security behaviors [23].

Facebook is a platform where users interact with their friends and family members. Therefore, users may tend to share information and adjust their behaviors based on the perceived expectations of others. We define subjective norms as individuals' perceptions of the social pressure to perform or not perform a behavior related to online privacy and security, and conceptualize it as an interpersonal factor that may influence behavior.

3.1.3. Privacy concern. The stronger a user's concerns are about his/her privacy and/or security, the more likely the individual is to improve his/her security and/or disclose less personal information. Privacy concern is also likely to be influenced by the individual's cultural values [37]. Therefore, we defined the attitude in our model as the degree of concern users have about their online privacy and security on OSNs, and we conceptualized it as an intrapersonal factor.

The scale used to measure privacy concern of Internet users was created by modifying prior privacy concern instruments in the literature for three specific privacy concern constructs: control, collection, and awareness [37]. We adapted the questions to fit our study (e.g., the word "Internet" was changed to "Facebook").

3.1.4. Internet literacy. Ajzen [1] argued that the PBC and self-efficacy constructs were interchangeable. However, it was suggested that self-efficacy was more concerned with cognitive perceptions of control based on

internal control factors than with general, external factors [2]. Later studies [15] [10] suggested the use of measures of self-efficacy instead of PBC to predict intentions and behavior. It was found that self-efficacy also played a critical role in predicting information security behavior [7]. However, Internet technologies, such as OSNs, may be challenging even to technically capable users [13]. Therefore, we used the construct of Internet literacy rather than Internet self-efficacy to predict users' behavior because the latter construct only measures individuals' perceptions of their capabilities to perform a certain task [13].

Using Dinev and Hart's [12] definition, we refer to Internet literacy as the knowledge and skills required by the individual to use Internet applications efficiently for communication, entertainment, and work purposes, and to handle harmful content such as spam and phishing. We used Dinev and Hart's [12] Internet literacy scale without any modification.

We conducted an exploratory factor analysis (EFA) to uncover the underlying structure of Internet literacy, and we observed two dimensions under this variable. We found that two items addressed the generic skills that are necessary to use Facebook, whereas the other two focused on the technical skills required by users to protect their online accounts. To apply Internet literacy to the context of this study, we broke it down into two constructs: general Internet literacy and technical literacy. We assumed that general Internet literacy, such as how to use discussion boards, was relevant to privacy behavior, and that technical literacy, such as how to detect viruses, was relevant to security behavior. We conceptualized both literacies as intrapersonal factors.

3.1.5. Behavioral intention and behavior. We identified two areas in the information security literature that applied the TPB: 1) information disclosure and 2) protective behavior (e.g., use of security controls and settings [47]). We defined information disclosure as the decision one makes to disclose personal information on OSNs and protective behavior as the use of security controls, settings and the decisions that one makes to improve security. We chose information disclosure and password behavior to represent privacy behavior security behavior, respectively.

The scales for subjective norms, two behavioral intentions and behaviors were constructed in accordance with the TPB questionnaire guidelines that Fishbein and Ajzen [18] presented for behavioral prediction and adopting questions from previous relevant literature.

3.2. Data collection

We examined the espoused national cultural values in a single country because testing the model in multiple countries could override the effect of individualism and collectivism due to various national level influences. For example, Krasnova and Veltri [32] examined Germany and the U.S., two countries that had different individualist values based on Hofstede's cultural dimensions [24]. Although the U.S. had a higher individualism score and was expected to disclose less information compared to Germany, they found that information disclosure was significantly higher in the U.S. They tested the mediating effect of *uncertainty avoidance* on the relationship between privacy concern and self-disclosure. They found that the negative impact of privacy concern on self-disclosure was stronger in Germany, an uncertainty avoiding culture, than in the U.S., an uncertainty tolerant culture. Therefore, it is possible that the difference resulted due to other factors (e.g., higher level of uncertainty avoidance in Germany could have nullified the effect of individualism).

Data were collected using Amazon Mechanical Turk (MTurk). In order to increase the quality of the data, we took the following precautions: We accepted MTurk users to participate our study only if they had more than 5,000 *Human Intelligence Tasks (HIT) approved, 98% HIT approval rate*, and they were located in the U.S. An attention-check question (see Appendix D in the online appendix) was included to ensure that the participants paid attention to the instructions and the survey questions. Participants who failed to answer the attention-check question were not allowed to continue the survey. In addition, we included *Qualtrics*' time stamps feature to record the length of time a participant spent on each survey page. Unrealistic responses (e.g., answering 20 questions less than 10 seconds) were excluded from the analyses. We collected 250 responses; however, the final sample size was 182 after the responses were screened based on the timestamps and deleting the incomplete survey responses were deleted.

The participants' ages ranged from 21 to 80 years, with a mean of 38.82 years (*SD* = 13.26). 54.9% were female and 45.1% were male. Two thirds of the participants (65.9%) at least had two-year college degree or higher. Most of the participants (89.6%) had a Facebook profile for more than three years, with a mean of 6.48 years (*SD* = 2.38). The number of Facebook friends of the participants ranged from 10 to 3,878, with a mean of 291.42 friends (*SD* = 413.28).

3.3. The measurement model

The test of the measurement model included the estimation of the construct validity and reliability of the measures. Construct validity was examined by assessing the standardized factor loadings of items in the model. A principal axis factoring analysis using varimax rotation extracted 12 factors that cumulatively explained 59% of the variance in the data. It was suggested that each item

should have a minimum factor loading of .60 on its hypothesized construct [42]. This norm was set for 46 of 57 items. Four items had loadings of .523, .565, .545, and .576 respectively, but were reasonably close to the suggested minimum factor loading and hence were included. One item in the vertical collectivism construct had a loading of .316. However, because the question made theoretical sense, it was included. Six items did not meet the criterion, so they were subsequently dropped.

The scale reliabilities were measured using Cronbach's alpha. The Cronbach's alpha of all the constructs was greater than .7, thus, providing a satisfactory level of reliability. Table 2 presents the results of reliabilities and validities of each construct.

Table 2. Instrument reliabilities and validities*

Construct	Variable	Mean	*SD*	Cronbach Alpha	Factor Loadings
Privacy	PC_01	4.69	1.74	.963	.900
Concern	PC_15	5.56	1.36		.672
Social	SN_01	4.59	1.65	.887	.886
Norm	SN_07	5.02	1.47		.523
Literacy:	IL_01	5.26	1.79	.706	.775
General	IL_02	5.69	1.54		.770
Literacy:	IL_03	5.51	1.76	.829	.682
Virus	IL_04	5.40	1.79		.682
Privacy	PB_01	6.03	1.18	.815	.906
Behavior	PB_05	5.98	1.20		.545
Security	SB_01	5.98	1.44	.727	.744
Behavior	SB_04	4.84	2.24		.576
Horizontal	HC_01	3.83	.79	.755	.830
Collectivism	HC_04	3.65	.97		.655
Vertical	VC_01	3.68	1.03	.715	.810
Collectivism	VC_04	3.66	.82		.316
Horizontal	HI_01	3.84	.94	.743	.792
Individualism	HI_04	4.16	.76		.670
Vertical	VI_01	2.36	1.08	.757	.773
Individualism	VI_04	2.51	1.11		.706

* Due to space constraints, only items with the highest and the lowest factor loadings for each construct are reported. The complete table can be found in Appendix C in the online appendix.

4. Analyses and results

4.1. The results of correlation

Table 3 shows the means and standard deviations (*SD*) for the key variables, and the correlation matrix for estimating the recursive model hypothesized in this study. As shown in Table 3, the intention for privacy was positively correlated with intention for security (r = .32, p < .01). However, we did not find a significant correlation between privacy and security behaviors (r = .08, p > .05). This finding confirms our argument that individuals who are motivated to protect their security may also intend to be cautious regarding their privacy; however, two behaviors might not align with each other.

According to the TPB, intention and behavior should be strongly correlated with each other [1]. We found that intention for privacy was positively correlated with privacy behavior (r = .49, p < .01). However, such relationship was not found between intention for security and security behavior (r = .11, p > .05). Interestingly, we observed a significant correlation between intention for security and privacy behavior (r = .29, p < .01). It seems a gap exists between intention for security and security behavior. In other words, one's intention for security does not necessarily mean that he/she will perform the behavior. Thus we decided to run path analysis to determine whether any other factors could explain and predict security behavior.

4.2. Differences among dimensions of INDCOL

We examined the differences among four dimensions of INDCOL using a one-way between subjects analysis of variance (ANOVA). Each participant was assigned to one of the four groups based on the INDCOL scale.

Proposition 4 was not supported as we did not find any significant differences for subjective norms within or privacy behaviors between four groups. There were significant differences in security behavior among the four groups (F(3, 104) = 2.96, p < .05) and subjective norms (F(3, 104) = 3.70, p < .05) However, we did not

Table 3. Correlation matrix, means and standard deviations for the key variables

	1	2	3	4	5	6	7	8	9	10	11	12	Mean	SD
Vertical Individualist	1												2.88	.83
Horizontal Individualist	.22**	1											4.00	.64
Vertical Collectivist	.16*	.01	1										3.76	.68
Horizontal Collectivist	-.01	-.16*	.47**	1									3.81	.65
Subjective norms	.17*	-.14	.41**	.23**	1								4.88	1.22
Privacy Concern	.22**	.05	.18*	.16*	.50**	1							4.55	1.43
Literacy: Virus	.00	.07	.13	.09	-.13	-.01	1						5.47	1.46
Literacy: General	.02	-.01	.07	.02	-.07	-.09	.56**	1					5.45	1.64
Intention: Privacy	.14	.09	.23**	.17*	.25**	.47**	.01	-.09	1				5.03	1.68
Intention: Security	-.04	.11	.16*	.25**	.23**	.39**	.10	.06	.32**	1			4.73	1.72
Behavior: Privacy	-.12	.13	.22**	.21**	.14	.28**	.08	-.03	.49**	.29**	1		5.76	1.08
Behavior: Security	-.10	.18*	-.13	-.07	-.30**	-.11	.18*	.04	-.10	.11	.08	1	5.76	1.26

**p < .01, *p < .05

find any significant differences for other constructs. Thus, we ran post-hoc tests only for security behavior and subjective norms. We chose the *Gabriel pairwise test procedure* to test the mean difference for subjective norms due to the unequal sample size, and the *Games-Howell test* to analyze the mean differences in password behavior due to the unequal sample size and population variance in security behavior (*Levene* = 3.25, $df = 3$, $p < .05$) [16]. Although we found between group differences, the post hoc comparison test did not indicate a significant within group difference for subjective norms.

Proposition 3 was partially supported as we found significant difference for privacy behavior between VC and HI, but we did not find any significant differences in intrapersonal factors. The post hoc comparison using the *Games-Howell test* indicated that the mean score for password behavior among VC ($M = 4.97$, $SD = 1.50$) was significantly different than among HI ($M = 6.00$, $SD = .96$). However, the mean scores of HC and VI were not significantly different than HI and VC. This finding also partially confirmed *proposition 6*, that is, security behavior could show contrast depending on the sense of control and autonomy. VI represents the group that has a higher acceptance of control and group influence, whereas HI represents the opposite end. However, such contrast was not found for privacy behavior. In the following section, we will conduct path analysis to examine further the underlying mechanisms that cause this difference.

4.3. Path analysis results

We ran path analysis to test the model using AMOS 23.0. We treated both privacy and security behavior as dependent variables in our model as they take place on the same platform and if tested separately, the underlying mechanisms of these two behaviors might not be observed.

Each of the four dimensions of INDCOL was treated as an exogenous variable. The other eight variables in the model were treated as endogenous variables, including one interpersonal factor (subjective norms), three intrapersonal factors (privacy concern and two Internet literacy—general and virus respectively), intention for privacy and intention for security, and privacy behavior and security behaviors.

We followed the basic steps suggested by Kenny [29] to run the path analysis and achieve a good fit model. We first tested the model with both hypothesized and non-hypothesized paths. We deleted those non-significant paths with $p > .01$. Retaining the hypothesized and significant non-hypothesized paths from the previous step, we reran the model and deleted those hypothesized paths with $p > .05$. Finally, we reran the model and deleted all the non-significant paths with $p > .05$. We also used modification indices to achieve the most parsimonious model with a good model fit [30], $\chi^2 (41) = 51.89$ ($p > .05$), NFI = .89, TLI = .96, CFI = .97, and RMSEA = .04. In this model, 28% variance in privacy behavior and 13% variance in security behavior were explained. The final model with standardized path coefficients is presented in Figure 4. The R^2 for each endogenous variable is reported in parentheses.

The findings of the path analysis partially supported *propositions 1* and *2*, that are security behavior is predicted by intrapersonal (privacy concern and literacy) and privacy behavior is predicted by interpersonal factors (subjective norms). Although we could not find a direct relationship between subjective norms and intention for privacy or privacy behavior, subjective norms had a strong indirect effect on intention for privacy through privacy concern. We also found that virus literacy ($\beta = .12$, $p = .095$), had a positive direct effect on security behavior; however, the coefficient was marginally significant.

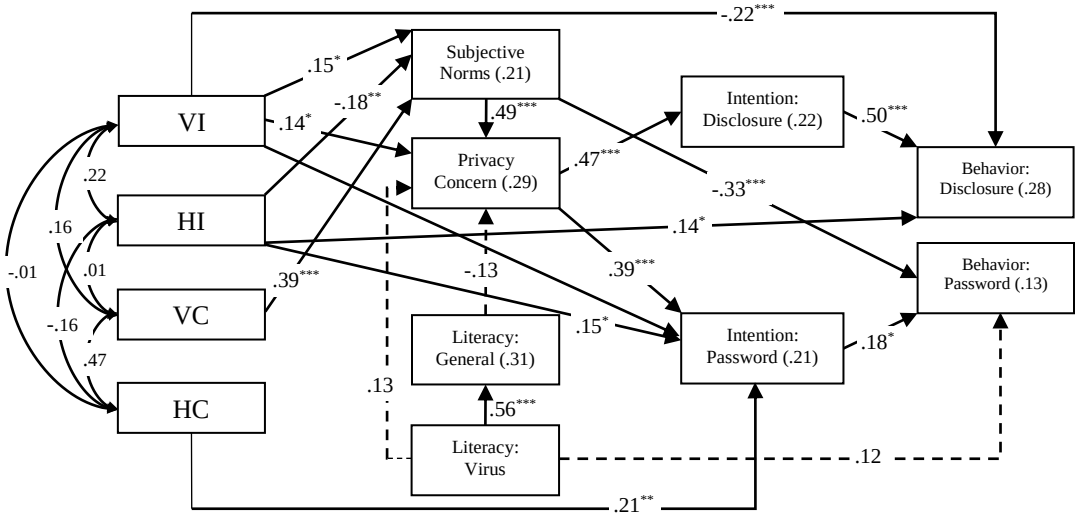

Figure 4. Hypothesized model and significance testing (*p < .001, **p < .01, *p < .05)**

Furthermore, subjective norms had a negative direct effect on security behavior (β = -.33, p < .001), implying that people who value what their close network thinks of them tend to have a weaker password. In fact, we found that VC and HI had opposite effects on subjective norms and security behavior, partially confirming *proposition 5*, that is users who have greater control may have stronger security behavior, and *proposition 6*, VC (β = .39, p < .001) had a positive while HI (β = -.18, p < .01) had a negative direct effect on subjective norms. VC had a negative indirect (β = -.13, p < .001) and HI had a positive indirect effect (β = .06, p < .01) on security behavior through subjective norms. Similar to the effect of VC, VI (β = .15, p < .05) had a positive effect on subjective norms and a negative indirect effect (β = -.02, p < .05) on security behavior through subjective norms. HC had a positive indirect effect (β = .04, p < .05) on security behavior through intention for security. Findings showed that VC and VI had negative, and HC and HI had positive indirect effects on security behavior, indicating that as the degree of individuals' acceptance of control increases, people tend to give up on their security.

VI and HI had a direct effect on privacy behavior while VC and HC did not have any direct or indirect effects on either intention for privacy or privacy behavior. However, effect of VI on privacy behavior was negative, meaning that individuals who have high levels of autonomy and acceptance of hierarchy disclose more information. This finding is in line with *proposition 5* that the acceptance of hierarchy causes individuals to relinquish their privacy to authority. The effect of HI on privacy behavior was positive, indicating that high autonomy and control cause less disclosure. This finding could explain the contradictory results on disclosure in the literature that individualism might not explain certain behavior, and its two dimensions could have different effects on information disclosure.

5. Conclusion

This study makes three contributions to the literature. First, online privacy and security behaviors are often used interchangeably and to the best of our knowledge there was no research devoted to explain to what extent and how these two behaviors vary from one another. This study highlights the subtle differences between privacy and security behaviors and calls attention that terminology of these two should be used with caution as we found that they were inherently distinct and affected differently by cultural characteristics and a set of factors.

Second, our findings addressed one possible reason for inconsistent results of the previous cross-cultural IS research. Examining online behaviors based on national culture or categorizing individuals under broad cultural values are simplistic and might be misleading [41]. To address this gap, we proposed a framework by coupling the grid-group theory and INDCOL scale that researchers can adopt for segmenting individuals with distinct cultural characteristics. Such segmentation would allow more accurate comparisons in cross-cultural research.

Finally, this study sheds light on the design and implementation of interventions, such as contextualized security trainings, warnings, and policies that aim to motivate individuals with diverse cultural backgrounds to adopt better privacy and security behaviors. We found the underlying distinct mechanisms of these two behaviors and identified predictors of each, which practitioners can target as the key determinants when promoting better privacy and security behaviors.

6. References

[1] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

[2] Bandura, A. (1992). On rectifying the comparative anatomy of perceived control: Comments on "Cognates of personal control". *Applied and Preventive Psychology, 1*(2), 121-126.

[3] Bansal, G., Zahedi, F., & Gefen, D. (2007). The impact of personal dispositions on privacy and trust in disclosing health information online. *AMCIS 2007 Proceedings*, 57.

[4] Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*(5), 313-324.

[5] Bond, R., & Smith, P. B. (1996). Culture and conformity: A meta-analysis of studies using Asch's (1952b, 1956) line judgment task. *Psychological Bulletin, 119*(1), 111.

[6] Cao, J., & Everard, A. (2008). User attitude towards instant messaging: the effect of espoused national cultural values on awareness and privacy. *Journal of Global Information Technology Management, 11*(2), 30-57.

[7] Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. (2006). Role of perceived importance of information security: An exploratory study of middle school children's information security behavior. *Issues in Informing Science and Information Technology, 3*, 127-135.

[8] Chen, C. C., Medlin, B. D., & Shaw, R. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security, 16*(4), 360-376.

[9] Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101.

[10] de Vries, H., Dijkstra, M., & Kuhlman, P. (1988). Self-efficacy: The third factor besides attitude and subjective norm as a predictor of behavioural intentions. *Health Education Research, 3*(3), 273-282.

[11] Dincelli, E., & Goel, S. (2015). Research design for study of cultural and societal influence on online privacy behavior. *IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop*, Newark, Delaware.

[12] Dinev, T., & Hart, P. (2004). Internet privacy, social awareness, and Internet technical literacy. An exploratory investigation. *BLED 2004 Proceedings*, 24.
[13] Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.
[14] Douglas, M. (1970). *Natural symbols: Explorations in cosmology*. London: Barrie and Rockliff.
[15] Dzewaltowski, D. A., Noble, J. M., & Shaw, J. M. (1990). Physical activity participation: Social cognitive theory versus the theories of reasoned action and planned behavior. *Journal of Sport & Exercise Psychology, 12*(4), 388-405.
[16] Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). Sage.
[17] Fire, M., & Puzis, R. (2012). Organization mining using online social networks. *Networks and Spatial Economics*, 1-34.
[18] Fishbein, M., & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach*. Taylor & Francis.
[19] Fisher, E. B., Brownson, C. A., O'Toole, M. L., Shetty, G., Anwuri, V. V., & Glasgow, R. E. (2005). Ecological approaches to self-management: the case of diabetes. *American Journal of Public Health, 95*(9), 1523-1535.
[20] Glanz, K., Rimer, B. K., & Viswanath, K. (2008). *Health behavior and health education: theory, research, and practice*: John Wiley & Sons.
[21] Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Workshop on Privacy in the Electronic Society*, 71.
[22] Gunatilaka, D. (2011). A survey of privacy and security issues in social networks. *IEEE INFOCOM Proceedings*, 27.
[23] Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.
[24] Hofstede, G. (1980). *Culture's consequences: International differences in work-related values*. Sage
[25] Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74-81.
[26] James, T. L., Warkentin, M., & Collignon, S. E. (2015). A dual privacy decision model for online social networks. *Information & Management, 52*(8), 893-908.
[27] Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An emprical study. *MIS Quarterly, 34*(3), 549-A544.
[28] Karahanna, E., Evaristo, J. R., & Srite, M. (2006). Levels of culture and individual behavior: An integrative perspective. *Advanced Topics in Global Info. Management, 5*(1), 30-50.
[29] Kenny, D. A. (1979). *Correlation and causality*. Wiley.
[30] Kline, R. B. (2010). *Principles and practice of structural equation modeling* (3rd ed.). The Guilford Press.
[31] Krasnova, H., & Veltri, N. F. (2010). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. *HICSS 2010 Proceedings*, 43.
[32] Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering, 4*(3), 127-135.
[33] Kwak, D.-H., Kizzier, D., Zo, H., & Jung, E. (2011). Understanding security knowledge and national culture: A comparative investigation between Korea and the US. *Asia Pacific Journal of Information Systems, 21*(3), 51-69.
[34] Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly, 30*(2), 357-399.
[35] Lili, W., & Min, D. (2014). Effect of cultural factors on online privacy concern: Korea vs. China. *Journal of Infirmation Technology Applications & Management, 21*(2), 149-165.
[36] Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27*(4), 163-200.
[37] Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.
[38] McLeroy, K. R., Bibeau, D., Steckler, A., & Glanz, K. (1988). An ecological perspective on health promotion programs. *Health Education & Behavior, 15*(4), 351-377.
[39] Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM, 38*(12), 65-74.
[40] Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35-57.
[41] Myers, M. D., & Tan, F. B. (2003). Beyond models of national culture in information systems research. *Advanced Topics in Global Information Management, 2*, 14-29.
[42] Nunnally, J. C. (1978). *Psychometric theory*. McGraw-Hill.
[43] Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems, 19*(2), 181-195.
[44] Schmidt, M. B., Johnston, A. C., Arnett, K. P., Chen, J. Q., & Li, S. (2008). A cross-cultural comparison of US and Chinese computer security awareness. *Journal of Global Information Management, 16*(2), 91.
[45] Singelis, T. M., Triandis, H. C., Bhawuk, D. P., & Gelfand, M. J. (1995). Horizontal and vertical dimensions of individualism and collectivism: A theoretical and measurement refinement. *Cross-cultural Research, 29*(3), 240-275.
[46] Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248-273.
[47] Taneja, A., Vitrano, J., & Gengo, N. J. (2014). Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation. *Computers in Human Behavior, 38*, 159-173.
[48] Triandis, H. C. (1995). *Individualism & collectivism*. Boulder, CO, US: Westview Press.
[49] Warkentin, M., Charles-Pauvers, B., & Chau, P. Y. K. (2015). Cross-cultural IS research: perspectives from Eastern and Western traditions. *European Journal of Information Systems, 24*(3), 229-233.
[50] Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management, 47*(2), 115-123.